Department of Defense

INSTRUCTION

NUMBER 2000.16

January 8, 2001

ASD(SO/LIC)

SUBJECT: DoD Antiterrorism Standards

References: (a) DoD Instruction 2000.16, "DoD Combating Terrorism Program Standards," July 21, 1997 (hereby canceled)
(b) DoD Directive 2000.12, "DoD Antiterrorism/Force Protection Program," April 13, 1999
(c) DoD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence," February 19, 1993
(d) DoD Instruction 5210.84, "Security of DoD Personnel at U. S. Missions Abroad," January 22, 1992
(e) through (j), see enclosure 1

1. REISSUANCE AND PURPOSE

1.1. This Instruction reissues reference (a), updates policy implementation, assigns responsibilities, and prescribes procedures under reference (b) for protection of personnel and assets from acts of terrorism.

1.2. Reference (c) assists the DoD Components to implement this Instruction and reference (b). Reference (d) provides guidance for security of personnel at overseas locations. Specific guidance for DoD elements and personnel under the responsibility of Department of State (DOS) is outlined in the DoD/DOS Memorandum of Understanding (MOU) reference (e). Reference (f) refers to specific common criteria and minimum construction standards to mitigate antiterrorism vulnerabilities and terrorist threats.

2. APPLICABILITY AND SCOPE

2.1. This Instruction applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the Department of Defense Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components"). The term "Services," as used herein, refers to the Army, the Navy, the Air Force, the Marine Corps, and the Coast Guard.

2.2. The standards in this Instruction apply only to the DoD Antiterrorism (AT) portion of the Force Protection (FP) program.

3. DEFINITIONS

Terms used in this Instruction are defined in enclosure 2.

4. POLICY

It is DoD policy:

4.1. To protect DoD personnel, their families, installations, facilities, information and other material resources from terrorist acts.

4.2. To establish primary standards for AT efforts of the Department of Defense, supplemented by guidance contained in DoD O-2000.12-H (reference (c)).

4.3. That Commanders at all levels have the authority to enforce security measures and are responsible for protecting persons and property subject to their control. Nothing in this Instruction shall detract from, or conflict with, the inherent and specified authorities and responsibilities of the DoD Components and Commanders.

5. RESPONSIBILITIES

By authority of DoD Directive 2000.12 (reference (b)), the following responsibilities are delineated:

5.1. The Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, under the Under Secretary of Defense (Policy), shall:

5.1.1. Provide AT policy oversight and ensure compliance with this Instruction by all Department of Defense Components, both within and outside the United States.

5.1.2. Develop, publish, and maintain this Instruction to provide standards for protective measures that serve to reduce the vulnerability of Department of Defense personnel and their families to terrorist acts.

5.1.3. Be the point of contact for the Department of Defense with the Department of State (DOS) for the standards contained in this Instruction and be responsible at the departmental level for resolving with the Department of State any conflicts between any DoD Component and any United States Country Team with respect to such standards.

5.2. The Heads of the DoD Components shall:

5.2.1. Ensure compliance with this Instruction.

5.2.2. Identify the level of command (i.e., the specific subordinate commanders) required to meet these standards.

6. PROCEDURES

All DoD Components shall utilize the definitions in enclosure 2 and the standards contained in enclosure 3 to implement the DoD AT policies within their organizations.

7. INFORMATION REQUIREMENTS

The review, assessment, and reporting of AT programs is exempt from licensing in accordance with paragraphs C4.4.1., C4.4.2., C4.4.7., and C4.4.8. of DoD 8910.1-M (reference (i)).

8. EFFECTIVE DATE

This Instruction is effective immediately.

Brian E. Sheridan
Assistant Secretary of Defense for
Special Operations and Low-Intensity Conflict

Enclosures - 3
- E1. References, continued
- E2. Definitions
- E3. Department of Defense Antiterrorism (AT) Standards

E1. ENCLOSURE 1

REFERENCES, continued

(e) Memorandum of Understanding Between the Department of State and the Department of Defense on Security on the Arabian Peninsula, September 15, 1996, and subsequent State-DoD Memorandum of Understanding on Security, December 16, 1997, applicable worldwide

(f) Interim Department of Defense Antiterrorism/Force Protection (AT/FP) Construction Standards Memorandum, December 16, 1999

(g) Department of Defense Deputy Directorate for Operations (Combating Terrorism) J-34, AT/FP Planning Template CD-ROM and Weapons of Mass Destruction (WMD) Appendix

(h) Joint Pub 3-07.2, "Joint Tactics, Techniques, and Procedures for Antiterrorism," March 17, 1998

(i) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 30, 1998

(j) Defense Threat Reduction Agency (DTRA) Force Protection Security Classification Guide, Joint Staff Integrated Vulnerability Assessment Program, August 2000

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Antiterrorism (AT). Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces. The AT program is one of several security-related programs that fall under the overarching Force Protection and Combating Terrorism programs. An AT program is a collective effort that seeks to reduce the likelihood that Department of Defense affiliated personnel, their families, facilities, and materiel will be subject to a terrorist attack, and to prepare to respond to the consequences of such attacks should they occur.

E2.1.2. Antiterrorism Plan (AT Plan). An AT Plan is the specific measures taken to establish and maintain an AT Program.

E2.1.3. Antiterrorism Officer (ATO). The installation and/or regional, or facility AT advisor charged with managing the AT Program.

E2.1.4. Combating Terrorism (CbT). Combating terrorism within the Department of Defense encompasses all actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts), counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), terrorism consequence management (preparation for and response to the consequences of a terrorist incident/event), and intelligence support (collection and dissemination of terrorism-related information) taken to oppose terrorism throughout the entire threat spectrum, to include terrorist use of chemical, biological, radiological, nuclear materials or high-yield explosive devices (CBRNE).

E2.1.5. Counterterrorism (CT). Offensive measures taken to prevent, deter, and respond to terrorism.

E2.1.6. Department of Defense (DoD) Terrorism Threat Analysis Methodology. See DoD O-2000.12-H (reference (c)) for an explanation of the DoD Terrorism Threat Analysis Methodology.

E2.1.7. Force Protection (FP). Security programs designed to protect service members, civilian employees, family members, facilities, information, and equipment in all locations and situations, accomplished through the planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs.

E2.1.8. High-Risk Billet. Authorized personnel billet (identified and recommended by appropriate authority) that because of grade, assignment, travel itinerary, or symbolic value may make personnel filling them an especially attractive or accessible terrorist target.

E2.1.9. High-Risk Personnel. Personnel who, by their grade, assignment, symbolic value, or relative isolation are likely to be attractive or accessible terrorist targets.

E2.1.10. Terrorism. The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies, in the pursuit of goals that are generally political, religious, or ideological.

E2.1.11. Terrorism Consequence Management (TCM). Department of Defense preparedness and response for mitigating the consequences of a terrorist incident including the use of a weapon of mass destruction. Department of Defense consequence management activities are designed to support the lead Federal Agency (domestically, Federal Emergency Management Agency (FEMA); overseas, DOS) and include measures to alleviate damage, loss of life, hardship or suffering caused by the incident; protect public health and safety; and restore emergency essential Government services.

E.2.1.12. Terrorist Incident Response Measures. A set of procedures in place for response forces to deal with the effects of a terrorist incident.

E2.1.13. Terrorism Threat Assessment. The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat. Also, it is the product of a threat analysis for a particular unit, installation, or activity.

E2.1.14. Terrorist Threat Conditions. A Chairman of the Joint Chiefs of Staff-approved program standardizing the Military Services' identification of and recommended responses to terrorists threats against U.S. personnel and facilities. This program facilitates inter-Service coordination and support for antiterrorism activities. Also called THREATCONS.

E2.1.15. Terrorism Threat Analysis. In antiterrorism, threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target a facility. A threat analysis will review the factors of the presence of a terrorist group, operational capability, activity, intentions, and operating environment.

E2.1.16. Vulnerability.

E2.1.16.1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or will to fight diminished.

E2.1.16.2. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment.

E2.1.17. Vulnerability Assessment. The process through which the commander determines the susceptibility to attack and the broad range of physical threats to the security of personnel and facilities, which provides a basis for determining antiterrorism measures that can protect personnel and assets from terrorist attacks.

E2.1.18. Weapons of Mass Destruction (WMD). Any weapons or device that is intended, or has the capability of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Can be nuclear, chemical, biological, radiological, or large explosive device weapons, but excludes the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon.

E3. ENCLOSURE 3

DoD ANTITERRORISM (AT) STANDARDS

E3.1.1. The AT Standards required to implement DoD policy are:

E3.1.1.1. DoD STANDARD 1: DoD AT Policy. Combatant Commanders, Chiefs of Service, and Directors of DoD Agencies and Field Activities (hereafter referred to collectively as "CINCs and/or Services and/or DoD Agencies") are responsible for the implementation of DoD AT policies within their organizations.

E3.1.1.2. DoD STANDARD 2: Development of AT Standards. CINCs and/or Services and/or DoD Agencies shall develop and implement a comprehensive AT program under their respective control to comply with all the standards contained in this Instruction. CINCs and/or Services and/or Agencies shall use standards contained herein as baseline standards. CINCs and/or Services and/or Agencies may promulgate unique requirements in their implementing directives to supplement the standards contained herein. As a minimum, these standards shall address the following areas:

E3.1.1.2.1. Procedures to collect and analyze terrorist threat information, threat capabilities, and vulnerabilities to terrorist attacks.

E3.1.1.2.2. Terrorism threat assessment, AT Plans, Terrorist Incident Response Measures, and Terrorist Consequence Management measures.

E3.1.1.2.3. Procedures to enhance AT protection.

E3.1.1.2.4. Procedures to identify AT requirements and to program for resources necessary to meet security requirements.

E3.1.1.2.5. Vulnerability Assessments; and

E3.1.1.2.6. Construction.

E3.1.1.3. DoD STANDARD 3: Assignment of AT Operational Responsibility. When antiterrorism responsibilities for the CINCs and/or Services and/or Department of Defense Agencies conflict or overlap, and are not otherwise governed by law, a specific Department of Defense policy, or an appropriate memorandum of agreement, the geographic CINC's force protection policies will take precedence over all force protection policies or programs of any DoD Component deployed in that command's area of responsibility (AOR) and not otherwise under the security responsibility of the Department of State.

E3.1.1.3.1. Commanders at all levels shall take appropriate measures to protect DoD personnel, families, facilities, and materiel, and reduce the vulnerability to terrorist use of WMD.

E3.1.1.4. <u>DoD STANDARD 4</u>: <u>AT Coordination in Overseas Locations</u>.

E3.1.1.4.1. CINCs and/or Services and/or DoD Agencies in overseas locations shall coordinate their AT efforts with host nation authorities and the U.S. Embassy, as appropriate. DoD Intelligence and Counterintelligence elements shall coordinate their activities in support of AT plans and programs through established DoD procedures. See reference (d).

E3.1.1.4.2. CINCs with geographic responsibilities shall coordinate AT matters with Chiefs of Missions (CoMs) for countries within their area of responsibility (AOR) and with functional CINCs and Department of Defense Agencies whose forces are stationed in or transit the geographic CINC's AOR. To ensure timely geographic CINC visibility of additional AT obligations, functional CINCs and DoD Agencies whose forces will station in or transit the AOR of a geographic CINC should initiate coordination of AT matters with the geographic CINC. See reference (d).

E3.1.1.4.3. DoD elements not under the force protection responsibility of a geographic CINC, by law or under provisions of a CINC-CoM MOA, shall comply with the State Department's Overseas Security Policy Board (OSPB) Security Standards. See references (d) and (e).

E3.1.1.4.4. The Director of the Defense Intelligence Agency (DIA), acting as the Department of Defense's executive agent for diplomatic security matters, through the United States Defense Representative (USDR), shall ensure that non-CINC-assigned DoD elements, whose AT responsibility rests with the CoM, comply with OSPB standards. See reference (d).

E3.1.1.4.5. In those countries covered by the Memorandum of Understanding (MOU) between the Department of State and the Department of Defense on Security of DoD Elements and Personnel in Foreign Areas (reference (e)), the designated DoD representative for resolution of disputes with Department of State officials is the Deputy Assistant Secretary of Defense for Combating Terrorism Policy and Support (CTP&S), or his designated representative. CINCs who have concerns about Department of State standards shall bring them to the attention of DASD(CTP&S) through the Chairman of the Joint Chiefs of Staff.

E3.1.1.5. DoD STANDARD 5: Comprehensive AT Development, Implementation, and Assessment. Commanders at all levels shall develop and implement a comprehensive AT program for personnel under their respective control designed to accomplish all the standards contained in this Instruction.

E3.1.1.5.1. AT Management. To develop and implement AT programs and plans, CINCs and/or Military Departments and/or Services and/or DoD Agencies shall designate a staff officer in writing to supervise, inspect, exercise, review, assess, and report on the installation AT programs within the theater or command.

E3.1.1.5.2. Elements of the Comprehensive AT Development, Implementation, and Assessment. AT program elements include threat assessments, planning, exercises, program reviews, training, and vulnerability assessments. The process, or sequence, of AT program elements should be iterative and serve continuously to refine the AT Plan.

E3.1.1.6. DoD STANDARD 6: Antiterrorism Officers (ATOs) shall be assigned in writing at each installation or base, as well as deploying organization (e.g., battalion, squadron, ship). Commanders shall designate a commissioned officer, non-commissioned officer, or civilian staff officer in writing as the ATO who shall be trained in AT procedures in a formal Service-approved Level II AT Training course.

E3.1.1.7. DoD STANDARD 7: Application of Department of Defense Terrorism Threat Analysis Methodology. Commanders shall use the Department of Defense Terrorism Threat Level classification system to identify the terrorism threat in a specific overseas country.

E3.1.1.7.1. The Department of Defense Terrorism Threat Level classification system is a set of standardized terms used to quantify the level of terrorism threat on a country-by-country basis. The Terrorism Threat Level terms are Low, Moderate, Significant, and High. The system evaluates the threat using a variety of analytical threat factors. See reference (c).

E3.1.1.7.2. The DIA sets the Department of Defense Terrorism Threat Level identifying the potential risk to DoD interests in a particular country. The Department of Defense Terrorism Threat Level applies whether or not U.S. personnel are present in the country. CINCs, with geographic responsibilities, may also set Terrorism Threat Levels for specific personnel, units, and installations in countries within the CINC's area of responsibility, using the definitions established by DIA. Commanders at all levels shall use their own threat analysis as the basis for developing plans and programs to protect assets within their AOR. Terrorism Threat Levels are estimates with no direct relationship to specific Threat Conditions (THREATCONs). A THREATCON is a security posture promulgated by the commander in consideration of a variety of factors (e.g., a terrorist threat analysis, Threat Level, etc.). Terrorism Threat Levels should not be confused with THREATCONs.

E3.1.1.7.3. Effective application of the Terrorism Threat Level classification system requires an integrated terrorism threat analysis, incorporating information collection and analysis from all sources, coupled with a thorough understanding of the threat analysis factors. Threat analysis factors must be viewed in the context of the specific security environment pertaining to individuals, deployed units, facilities and installations resident in the country being analyzed. An integrated terrorism threat assessment uses a variety of intelligence information about a specified terrorist group to determine an individual, unit, facility, and, or an installation's vulnerability to a specific form of terrorist attack. Thus, the threat analysis should be supported by intelligence gathering (overseas) and information gathering (domestically) on the part of appropriate authorities.

E3.1.1.8. <u>DoD STANDARD 8</u>: <u>Threat Information Collection and Analysis</u>. Commanders shall task the appropriate organizations under their command to gather, analyze, and disseminate terrorism threat information, as appropriate.

E3.1.1.8.1. Identifying the potential terrorism threats to DoD personnel and assets is the first step in developing an effective AT program. Commanders at all levels who understand the threat can assess their ability to prevent, survive, and prepare to respond to an attack.

E3.1.1.8.2. A Terrorism Threat Assessment requires the analysis of all available information on terrorist activities. In addition to tasking appropriate agencies to collect information, commanders at all levels can and should encourage personnel under their command to report information on individuals, events, or situations that could pose a threat to the security of DoD personnel, families, facilities, and resources.

E3.1.1.9. <u>DoD STANDARD 9</u>: <u>Threat Information Flow</u>. Commanders at all levels shall forward up and down the chain of command all information pertaining to suspected terrorist threats, or acts of terrorism involving DoD personnel or assets in their AOR.

E3.1.1.9.1. The pattern of terrorist surveillance, targeting and planning is best recognized through sharing of information. These efforts shall include the chain of command and the interagency process at the appropriate level.

E3.1.1.10. DoD STANDARD 10: Potential Threat of Terrorist Use of Weapons of Mass Destruction (WMD). Commanders at all levels shall take appropriate measures to protect DoD personnel, families, facilities, and materiel, and reduce the vulnerability to terrorist use of WMD. Thus, CINCs and/or Military Departments and/or Services and/or DoD Agencies shall develop estimates for potential terrorist use of WMD in their AOR.

E3.1.1.10.1. Reports through the chain of command shall be processed immediately when significant information is obtained identifying organizations with WMD capabilities operating in their AOR.

E3.1.1.11. DoD STANDARD 11: Adjustment of Threat Conditions (THREATCONs). Combatant Commanders have ultimate antiterrorism and force protection authority and responsibility within their AOR. Secretaries of the Services through the Service Chiefs are responsible for antiterrorism and force protection authority within the 48 contiguous States. Commanders at all levels shall develop a process, based on terrorism threat information and/or guidance from higher headquarters, to raise or lower THREATCONs.

E3.1.1.12. DoD STANDARD 12: THREATCON Measures Implementation. CINCs and/or Military Departments and/or Services and/or DoD Agencies shall ensure that THREATCON transition procedures and measures are properly disseminated and implemented by subordinate commanders within their AOR.

E3.1.1.13. DoD STANDARD 13: THREATCON Measures. Commanders at all levels shall develop site-specific measures or action tasks for each THREATCON that supplement those measures/actions enumerated for each THREATCON as listed within Appendix A of DoD O-2000.12-H (reference (c)). These measures will change as the threat situation increases from THREATCON Normal to THREATCON Delta.

E3.1.1.13.1. Commanders at all levels shall establish local measures to supplement reference (c) procedures to transition between THREATCONs. Whereas Terrorism Threat Levels are analytical assessments of terrorist activity in a country, THREATCONs are graduated categories of measures or actions commanders take to protect personnel and assets from attack.

E3.1.1.13.2. Commanders at all levels shall set a local THREATCON. Subordinate commanders may raise a higher level commander's THREATCON for their own area of operations. However, subordinate commanders shall not lower a higher level commander's THREATCON without the higher level commander's concurrence. Commanders shall ensure proper notifications are made.

E3.1.1.14. DoD STANDARD 14: Commanders shall maintain a comprehensive AT program for their AOR. Planning is critical to deterrence, detection, defense, and response to terrorist incidents. Where possible, Commanders may use as a guide the Department of Defense Deputy Directorate for Operations (Combating Terrorism) J-34, AT/FP Planning Template CD-ROM and Weapons of Mass Destruction (WMD) Appendix (reference (g)). The AT Plan and elements shall clearly describe site-specific AT measures. The AT Plan and elements should be written from the CINC level down to the installation level for permanent operations or locations, and incorporated in operations orders for temporary operations or exercises.

E3.1.1.14.1. At a minimum, the AT Plan shall address the following key elements. These key elements must be integrated into and/or support a comprehensive AT plan. Thus, stand-alone documents (e.g., Standard Operating Procedures, local regulations, or Operations Orders that articulate requirements for these key elements) shall be replicated in and/or referenced in the AT Plan. The AT Plan can also be a part of a stand-alone document:

E3.1.1.14.1.1. Terrorism Threat Assessment.

E3.1.1.14.1.2. AT Physical Security measures.

E3.1.1.14.1.3. Terrorist Incident Response measures.

E3.1.1.14.1.4. Terrorist Consequence Management measures.

E3.1.1.15. DoD STANDARD 15: Terrorism Threat Assessment. Commanders shall prepare a terrorism threat assessment for their AOR.

E3.1.1.15.1. CINCs and/or Services and/or DoD Agencies shall designate which subordinate commanders will prepare these terrorism threat assessments. This normally applies to installation commanders and above.

E3.1.1.15.2. The terrorism threat assessment is the tool that commanders use to arrive at a judgment of risk and consequences of terrorist attack. Commanders shall integrate threat information prepared by the intelligence community, technical information from security and engineering planners, and information from other sources to prepare their assessments. Commanders shall consider the factors of threat, criticality, and vulnerability of facilities, programs, and systems, as well as deterrence/response capabilities during the assessment process. Terrorism threat assessments shall be the basis and justification for recommendations on AT enhancements, program/budget requests, and the establishment of THREATCONs.

E3.1.1.16. DoD STANDARD 16: AT Physical Security Measures. AT Physical Security measures shall be considered, must support, and must be referenced within the AT Plan to ensure an integrated approach to terrorist threats. Where there are multiple commanders at an installation, the Installation Commander is responsible for coordinating and integrating individual unit physical security plans and measures into the AT Plan.

E3.1.1.16.1. The AT Physical Security measures shall integrate facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide maximum AT protection to personnel and assets. Well-designed AT Physical Security measures include detection, assessment, delay, denial, and notification. This is best accomplished through the development of a synchronized matrix that outlines who will do what, where, when, and how. These measures should include provisions for the use of physical structures: physical security equipment; chemical, biological, or radiological detection and protection equipment; security procedures; Random Antiterrorism Measures (RAMs); response forces; and emergency measures sufficient to achieve the desired level of AT protection and preparedness to respond to a terrorist attack.

E3.1.1.17. DoD STANDARD 17: Terrorist Incident Response Measures. Installation commanders shall prepare installation-wide terrorist incident response measures. These measures shall include procedures for determining the nature and scope of post-terrorist incidence response, and steps to reconstitute the installation's ability to perform AT measures.

E3.1.1.17.1. Terrorist Incident Response Measures should address the full scope of an installation's response to a terrorist incident. The nature of the response will depend on many factors. The character of operations underway at the time of the terrorist incident will have significant bearing on the scope, magnitude, and intensity of response.

E3.1.1.17.2. Inclusion of Off-Installation Personnel in AT Plans. Commanders shall ensure Terrorism Incident Response measures contain current residential location information for all assigned DoD personnel and their dependents, when stationed outside of the United States, territories and possessions in Moderate, Significant, and High Terrorism Threat Level areas. Such measures should provide for enhanced security and/or possible evacuation of DoD personnel and their dependents. Furthermore, commanders in Moderate, Significant, and High Terrorism Threat Level areas should investigate special security arrangements to protect DoD personnel and their dependents living on the civilian economy. Close coordination with other U.S. Government Agencies and the host nation is essential to ensure effective allocation of security resources and protection of DoD personnel.

E3.1.1.18. <u>DoD STANDARD 18</u>: <u>Terrorist Consequence Management Measures</u>. Although not an element of AT, Commanders shall include terrorist consequence management preparedness and response measures as an adjunct to the installation AT Plan. The Terrorist Consequence Management measures should include emergency response and disaster planning and/or preparedness to respond to a terrorist attack for installation and/or base engineering, logistics, medical, mass casualty response, transportation, personnel administration, and local and/or host nation support. In addition, special circumstances imposed by the nature of a terrorist attack may require broader analyses to include higher levels of authority or command. Terrorist use of weapons of mass destruction, or terrorist attacks on dignitaries while visiting DoD installations, will require immediate close coordination with higher command and the host nation and/or Federal, State and local authorities .

E3.1.1.19. <u>DoD STANDARD 19</u>: <u>Training and Exercises</u>. Commanders (ship, squadron, battalion-level and above) shall conduct field and staff training to exercise AT Plans, to include AT Physical Security measures, Terrorist Incident Response measures, and Terrorist Consequence Management measures, at least annually. AT exercises should be executed with the intent to identify shortfalls impacting the protection of personnel and assets against terrorist assault and subsequent consequence management efforts. To realize incorporation of lessons learned, commanders should maintain exercise documentation for no less than one year.

E3.1.1.19.1. Commanders (ship, squadron, battalion-level and above) shall ensure joint operations and/or exercises incorporate AT training and planning for forces involved.

E3.1.1.20. DoD STANDARD 20: Comprehensive AT Review. Commanders at all levels shall review their own AT program and plans at least annually to facilitate AT program enhancement. Furthermore, for the same purpose, commanders at all levels shall likewise review the AT Program and Plan of their immediate subordinate in the chain of command at least annually. While such reviews do not constitute a vulnerability assessment, they are intended to ensure compliance with the standards contained in this Instruction.

E3.1.1.20.1. To ensure the design and implementation of physical security measures coincident with the AT program are consistent with the local Terrorist Threat Level, AT programs shall also be reviewed when the Terrorism Threat Level changes.

E3.1.1.21. DoD STANDARD 21: General Requirements for AT Training. CINCs and/or Services and/or DoD Agencies shall ensure all assigned personnel receive appropriate training to advance AT awareness. Individual records shall be updated to reflect AT training in accordance with DoD Component policy.

E3.1.1.22. DoD STANDARD 22: Level I AT Awareness Training. CINCs and/or Services and/or DoD Agencies shall ensure that every military service member, DoD employee, and local national hired by the Department of Defense, regardless of rank, is made aware of the need to maintain vigilance for possible terrorist actions and employ AT tactics, techniques and procedures, as discussed in DoD O-2000.12-H and Joint Pub 3-07.2 (references (c) and (h)). Furthermore, the DoD Components shall offer Level I AT Awareness Training to contractor employees, under terms and conditions as specified in the contract.

E3.1.1.22.1. Individual security awareness and individual AT training are essential elements of an overall AT program. Each individual must be exposed at the earliest opportunity to share in the responsibility of ensuring alertness and the application of personal protection measures. Therefore, CINCs and/or Services and/or DoD Agencies shall provide Level I AT Awareness Training in basic training or in general military subject training for all initial entry Service and DoD Agency personnel.

E3.1.1.22.2. Thereafter, CINCs and/or Services and/or DoD Agencies shall provide Level I AT Awareness Training:

E3.1.1.22.2.1. Annually to all OCONUS-based DoD personnel.

E3.1.1.22.2.2. Annually to all CONUS-based DoD personnel who are eligible for OCONUS deployment. Active uniformed CONUS-based members of the CINCS and Services shall receive Level I training annually. Subsequently, DoD personnel deploying OCONUS shall be provided within 3 months of deployment an AOR update (refer to DoD STANDARD 23, below).

E3.1.1.22.2.3. Annually to all CONUS-based DoD personnel, regardless of duty status, if the CONUS Terrorism Threat Level is promulgated above "MODERATE."

E3.1.1.22.3. CINCs and/or Services and/or DoD Agencies shall ensure that every family member accompanying DoD personnel overseas is made aware of the need to maintain vigilance for possible terrorist actions and employ AT tactics, techniques, and procedures, as discussed in references (c) and (h). Thus, family members 14 years and older (or younger at the discretion of the DoD sponsor) traveling beyond CONUS on official business (i.e., on an accompanied permanent change of station move) shall receive Level I AT Awareness Training as part of their pre-departure requirements. Furthermore, the commander should encourage family members to receive Level I AT Awareness Training prior to any OCONUS travel (i.e., leave).

E3.1.1.22.4. Individuals may become qualified to administer Level I AT Awareness Training via two methods:

E3.1.1.22.4.1. Attending a formal Service-approved Level II ATO Training course of instruction. Such training must review current AT publications and identify methods for obtaining AOR-specific terrorism threat analyses, updates, and warnings.

E3.1.1.22.4.2. Commanders may qualify individuals who are subject matter experts and have received formal training in AT and individual protection (e.g., military and/or security police, special agents, etc., who have received specific formal training in AT tactics, techniques, and procedures). These individuals may be individually exempted by the Commander from the Level II ATO Training outlined in Table E3.T1. only if they receive additional training that reviews current AT publications and identifies the methods for obtaining AOR-specific updates.

E3.1.1.22.4.3. Table E3.T1. outlines Level I AT Awareness Training requirements.

E3.1.1.23. DoD STANDARD 23: AOR-Specific Training Requirements for all Department of Defense Personnel. CINCs with geographic responsibilities shall ensure that all DoD personnel entering their AOR have been provided access to AOR-specific information on AT protection.

E3.1.1.23.1. CINCs with geographic responsibilities have significant responsibilities for protecting personnel within their AOR. Individuals traveling outside CONUS for either permanent or temporary duty shall have completed annual Level I AT Awareness Training and shall have received a specific AOR update within three months prior to travel. CINCS, with geographic responsibilities, shall make AOR-specific AT protection information available to the DoD Components in support of this training. This information may be provided through multiple means including CINC publications, messages, and computer homepages. Losing CINCs and/or Military Departments and/or Services and/or DoD Agencies shall ensure that personnel departing to another CINC's geographical AOR shall be exposed to and execute the requirements of the gaining CINC's AOR-update.

E3.1.1.24. DoD STANDARD 24: Level II Antiterrorism Officer (ATO) Training. Level II ATO Training is designed to produce an AT advisor to the Commander. CINCs and/or Services and/or DoD Agencies shall ensure that each installation and/or deploying unit (e.g., battalion, squadron, ship) is assigned at least one Level II ATO trained individual.

E3.1.1.24.1. Table E3.T1. outlines Level II ATO training requirements.

E3.1.1.24.2. Level III Pre-Command AT Training. Level III Pre-Command AT Training is designed to expose the prospective commander to AT issues. Services and/or DoD Agencies shall ensure that pre-command training tracks provide Level III Pre-Command AT Training to prospective commanders.

E3.1.1.24.3. Table E3.T1. outlines Level III Pre-Command AT training requirements.

E3.1.1.24.4. Level IV AT Executive Seminar. The Level IV AT Executive Seminar is designed to expose senior Officers in the grades of O6-O8 and Department of Defense civilians in equivalent grades to AT issues.

E3.1.1.24.5. Table E3.T1. outlines Level IV AT Executive Seminar training requirements.

E3.1.1.24.6. Table E3.T1. describes training required by this standard.

Table E3.T1. Pre-deployment and Career Development AT Training Requirements

Level of Training	Target Audience	Minimum Training Standard
Level I AT Awareness Training provided annually to: (1) All OCONUS-based DoD personnel (2) All Active uniformed CONUS-based members of the CINCS and Services (3) All CONUS-based DoD personnel eligible for official OCONUS travel on Government orders (4) All CONUS-based DoD personnel regardless of duty status if the CONUS Terrorism Threat Level is promulgated above "MODERATE". **Graduates will have requisite knowledge to remain vigilant for possible terrorist actions and employ AT tactics, techniques, and procedures, as discussed in DoD O-2000.12-H (reference (c)) and Joint Pub 3-07.2 (reference (g)).	DoD personnel Accessions during initial Training. Military, Department of Defense Civilians, their family members 14 years old and greater (when family members are deploying or traveling on government orders), and DoD-employed Contractors.	Component-provided instruction incorporates Component-standardized POI consisting of the following minimum topics: 1. Viewing the Service-selected personal awareness video provided under the instruction of a qualified Level I AT Awareness instructor and/or DoD-sponsored, and Component-certified, computer-based and/or distance learning (DoD personnel accessions must receive initial training under instruction of a qualified Level I AT Awareness Instructor). 2. Instruction on the following: Introduction to Terrorism • Terrorist Operations • Individual Protective Measures Terrorist Surveillance Techniques • Improvised Explosive Device (IED) Attacks Kidnapping & Hostage Survival • Explanation of Terrorism Threat Levels and THREATCON System 3. Issuance of JS Guide 5260 "Service Member's Personal Protection Guide: A Self-Help Handbook to Combating Terrorism" and "Antiterrorism Individual Protective Measures" folding card. (Local reproduction of both is authorized.) 4. Receipt of AOR updates three months prior to travel to include current threat brief and AOR specific requirements as provided by the receiving geographic CINC.

Level of Training	Target Audience	Minimum Training Standard
Level II AT Officer (ATO) Training ** Graduates shall have requisite knowledge and materials to manage a comprehensive AT Program and advise the commander in all AT areas.	Officers/NCOs/civilian staff officers, who are tracked and command-designated to serve as the AT advisor to the Commander and provide Level I Instruction in coded billets.	Component-provided instruction (resident or MTT); incorporates Component-standardized POI consisting of the following minimum topics: • Understanding AT Roles and Responsibilities - Understand Policy & Standards - Access Reference Sources • Organize for AT - Command/Staff Relationships - FP Working Groups • Assess Vulnerabilities - Baseline Unit FP Posture - Conduct Assessment • Assess Threat - Intel/CI Integration - Information OPS • Create and Execute AT Programs - Use of Terrorism Threat Level/THREATCONs - Unit/Installation Protective Measures - Mitigating Vulnerabilities • Prepare AT Plans - Templates & Planning Tools - How to Develop & Write Plans - WMD Considerations - Use of RAM to protect the Installation • AT Resource Management - Requirements Generation & Prioritization - CbT RIF • Conduct AT Training - Exercise Unit AT Plans - Obtain AOR-specific updates - Oversee AT Level I Training 2. Review of DoD Directive 2000.12, Instruction 2000.16, Order 2000.12-H and other applicable Department of Defense/ Service/Agency publications. 3. Methods available for obtaining AOR-specific updates for deployment/travel areas. 4. Component-directed modules on other aspects of AT such as physical security requirements, technology updates, etc.

Level of Training	Target Audience	Minimum Training Standard
Level III Pre-Command AT Training **Graduates shall have requisite knowledge and materials to supervise a comprehensive AT Program and manage AT issues.	O-5/O-6 Commanders	Component-provided instruction during pre-command pipelines; incorporates Component-standardized POI consisting of the following minimum topics: 1. Viewing the SECDEF/CJCS Video 2. Directive/reference review • Understanding AT Responsibilities - Understanding Policy - Assessments - Off-Installation Housing • Ensuring Preparation of AT Plans - Baseline FP Posture - Mitigating WMD Attack - MOUs/MOAs • Ensuring Conduct of AT Planning - AT Plans & Training - Level I Training • Organizing for AT • Understand the Local Threat Picture - Fusion of Intelligence • Building a Sustainable AT Program - Terrorism Threat Levels • Executing Resource Responsibilities - AT Resource Programming - Construction Standards • Understanding Use of Force and ROE 3. Review of DoD Directive 2000.12, Instruction 0-2000.16, Handbook 2000.12-H, and other applicable Department of Defense/Service/Agency publications. 4. Issuance of Commander's Handbook (Joint Pub 5260).
Level of Training	Target Audience	Minimum Training Standard
Level IV AT Executive Seminar **Graduates shall have requisite knowledge and materials to provide oversight to AT Programs and Policies.	Officers in the grade of O6-O8 and Department of Defense civilians in equivalent grades selected by Services/CINCs/Department of Defense Agencies who are responsible for AT programs or involved in AT policy, planning and execution.	CJCS Executive-level seminar hosted by J-34. Provides pertinent current updates, briefings, and panel discussion topics. Seminar includes 3 tabletop AT wargames aimed at facilitating interaction and discussion among seminar participants.

E3.1.1.24.7. Commanders at all levels who receive individuals that are not properly trained shall, in the interest of force protection, provide the required AT training as soon as practicable upon the gain. Concurrently, they shall report the deficiency through their Department of Defense Component chain of command. The Department of Defense Component shall subsequently notify the providing commander and ensure appropriate measures are generated to prevent reoccurrence of the discrepancy.

E3.1.1.25. DoD STANDARD 25: Training for High-Risk Personnel and High-Risk Billets. CINCs and/or Services and/or DoD Agency Heads have been given substantial AT responsibilities for DoD personnel in their AORs assigned to high-risk billets or at high risk to terrorist attack. High Risk personnel are eligible for advanced AT training. In some instances, this training may be extended to include family members.

E3.1.1.25.1 The Services shall ensure personnel designated as PERSONNEL AT HIGH RISK TO TERRORIST ATTACK and PERSONNEL ASSIGNED TO HIGH-RISK BILLETS receive appropriate AT training. To this end, CINCs with geographic responsibilities shall communicate high-risk positions and high-risk personnel to their Service authority for AT, not less than annually to enable the Services to provide for the requisite training.

E3.1.1.25.2. Whenever possible, this appropriate AT training of designated personnel should be conducted by the Services prior to arrival in theater.

E3.1.1.26. DoD STANDARD 26: Vulnerability Assessments of Installations.

E3.1.1.26.1. Assessment Focus. Vulnerability Assessments shall focus on the assessed unit's overarching AT program. Antiterrorism programs should be subject to continual assessment to avoid complacency and to gain benefit from experience from other assessments. Evolving terrorism threats, changes in security technology, development and implementation of alternative concepts of peacetime operations, and changing local conditions make periodic assessments essential. Vulnerability assessments will normally occur at the installation commander level and above. These assessments should consider the range of identified and projected terrorism threats against a specific location or installation personnel, facilities and other assets. The assessment should identify vulnerabilities and solutions for enhanced protection of DoD personnel and resources.

E3.1.1.26.2. AT vulnerability assessments provide a vulnerability-based analysis of an activity's AT program. The assessment identifies, for the commander, vulnerabilities that may be exploited by terrorists and suggests options that may eliminate or mitigate those vulnerabilities. Information derived from vulnerability assessments will be classified in accordance with the Defense Threat Reduction Agency (DTRA) Security Classification Guide. See reference (j).

E3.1.1.26.3. Local Vulnerability Assessments. Local commanders shall conduct a local vulnerability assessment for facilities, installations, and operating areas within their area of responsibility. The local vulnerability assessment shall address the broad range of physical threats to the security of personnel and assets and shall be conducted at least annually.

E3.1.1.26.4. Higher Headquarters Vulnerability Assessments. CINCs and/or Military Departments and/or Services and/or DoD Agencies shall ensure lower level AT programs receive a Higher Headquarters Vulnerability Assessment at least once every three years to ensure unity of AT efforts throughout their AORs or subordinate commands. To provide essential visibility, commanders shall prioritize, track, and report vulnerabilities identified during vulnerability assessments to the next General Officer/Flag Officer or equivalent.

E3.1.1.26.5. For installations shared by CINCs and/or Services and/or DoD Agencies, a Higher Headquarters Vulnerability Assessment of the installation satisfies the three-year periodicity requirement for subordinate commands and/or tenants and/or detachments co-located within the confines of the assessed installation.

E3.1.1.26.6. Higher Headquarters Vulnerability Assessments satisfy the annual requirement for a Local Vulnerability Assessment.

E3.1.1.26.7. AT Site Criteria. Higher Headquarters Vulnerability Assessments shall be conducted at DoD Components, housing areas, facilities, and/or activities at locations and command levels identified as "installations." For the purpose of this Instruction, the following defines an assessment-eligible installation:

E3.1.1.26.7.1. Any DoD facility consisting of 300 or more personnel on a daily basis; and

E3.1.1.26.7.2. Any DoD facility bearing responsibility for emergency response and physical security plans and programs; and

E3.1.1.26.7.3. Any DoD facility possessing authority to interact with local non-military or host nation agencies or having agreements with other agencies or host nation agencies to procure these services.

E3.1.1.26.7.4. However, Higher Headquarters Vulnerability Assessments may be conducted at any DoD Component Activity when CINCs and/or Services and/or Agencies identify a time critical requirement or emergent need.

E3.1.1.26.8. AT Assessment Functional Areas. AT Vulnerability Assessments shall assess as a minimum the following functional areas:

E3.1.1.26.8.1. AT Plans and Programs. The assessment shall examine the assessed installation's AT program and ability to accomplish appropriate standards contained in this Instruction and/or applicable prescriptive standards established by the appropriate Combatant Command, Service, or DoD Agency.

E3.1.1.26.8.2. Counterintelligence, Law Enforcement Liaison, and Intelligence Support. The assessment shall focus on the ability to receive threat information and warnings from higher headquarters and local resources, actively collect information on the threat (when permitted and in accordance with applicable law and regulations), process that information to include local fusion and analysis, and develop a reasonably postulated threat statement of the activity. Further, the assessment will examine the ability to disseminate threat information to subordinate commands, tenant organizations, assigned or visiting DoD personnel (including military members, civilians, and contractor employees, and dependents), and how that process supports the implementation of appropriate force protection measures to protect military personnel, DoD civilians and family members.

E3.1.1.26.8.3. AT Physical Security Measures. The assessment shall determine the assessed unit's ability to protect personnel by detecting or deterring terrorists, and failing that, to protect by delaying or defending against acts of terrorism. Physical security techniques include procedural measures such as perimeter security, security force training, security surveys, medical surveillance for unnatural disease outbreaks, and armed response to warning or detection as well as physical security measures such as fences, lights, intrusion detection devices, access control systems, closed circuit television cameras, personnel and vehicle barriers, biological, chemical and radiological agent detectors and filters, and other security systems. The assessment should also consider commercial-off-the-shelf AT technology enhancements and potential solutions for those circumstances where existing technology or procedural modifications do not provide satisfactory solutions.

E3.1.1.26.8.4. Vulnerability to a Threat and Terrorist Incident Response Measures. The assessment shall examine the assessed unit's ability to determine its vulnerabilities against commonly used terrorist weapons and explosive devices, to include weapons of mass destruction. The assessment shall further examine the ability to provide structural or infrastructure protection against terrorist events. The ability to respond to a terrorist event, with emphasis on a mass casualty situation, shall also be examined.

E3.1.1.26.8.5. Vulnerability Assessments for Terrorist Use of WMD. The assessment shall assess the vulnerability of installations, facilities, and personnel within their AOR to terrorist use of WMD, to include the potential use of chemical, biological, nuclear or radiological agents.

E3.1.1.26.8.6. The assessment shall examine written plans and/or programs in the areas of counterintelligence, law enforcement liaison, intelligence support, security and post-incident response (the ability of the activity to respond to a terrorist incident, especially a mass casualty event, to include a disease outbreak caused by terrorist use of biological weapons).

E3.1.1.26.8.7. The assessment shall focus on the most probable terrorist threat for the facility and appropriate countermeasures. In cases where no identified threat exists, units shall be assessed on their ability to implement AT measures under increasing THREATCONs in response to an increase in the Terrorist Threat Level or terrorist threat warning.

E3.1.1.26.8.8. The assessment shall examine the availability of resources to support plans as written and the frequency and extent to which plans have been exercised.

E3.1.1.26.8.9. The assessment shall examine the degree to which plans complement one another and support the assessed unit's ability to identify changes in the terrorist threat, react to threat changes by implementing appropriate AT measures and provide an appropriate response should a terrorist event occur.

E3.1.1.26.8.10. Host Nation, Local Community, Inter-Service, and Tenant Support. The assessment shall examine the level and adequacy of support available to the activity from the host nation, local community, and where appropriate, inter-Service and tenant organizations to enhance force protection measures or respond to a terrorist incident.

E3.1.1.26.8.11. The assessment shall determine the integration and feasibility of plans with the host nation, local community and inter-Service and tenant organizations to provide security, law enforcement, fire, medical and emergency response capability in reaction to a terrorist event with emphasis on mass casualty situations.

E3.1.1.26.8.12. The assessment shall determine the adequacy of resources available to execute agreements and the extent and frequency to which plans are exercised.

E3.1.1.26.8.13. The assessment shall determine the status of formal and informal agreements with supporting organizations via Memorandums of Understanding or Agreement, Inter-Service Support Agreements, Host-Tenant Support Agreements, or other models.

E3.1.1.26.8.14. Site-Specific Characteristics. Site-specific circumstances may require assessment of additional functional areas. These additional requirements shall be as directed by the CINC and/or Service and/or DoD Agency creating the team and should be based on site-specific characteristics such as Terrorism Threat Level, terrorist characteristics, geography, and security environment.

E3.1.1.26.9. Team Composition and Level of Expertise. As a minimum, the level of expertise and team composition must support the assessment of the functional areas described above. Team membership shall have expertise in the following areas: physical security; civil, electrical, or structural engineering; special operations; operational readiness; law enforcement and medical operations; infrastructure; intelligence/counterintelligence, and consequence management. In exceptional cases, commanders may be required to tailor team composition and scope of the assessment to meet unique requirements of a particular site, but must meet the intent of providing a comprehensive assessment.

E3.1.1.26.9.1 Specific size and certification of expertise shall be as directed by the CINC and/or Service and/or DoD Agency creating the team. However, team members must be functionally orientated and have experience in the assessment area to be considered for team membership.

E3.1.1.26.9.2. Based on site-specific factors such as Terrorism Threat Level, terrorist characteristics, geography and security environment, assessment teams may be augmented by personnel with expertise in the areas of linguistics; chemical, biological, radiological weapons effects; AT technology; explosive ordnance disposal; special warfare; communications; information assurance or operations;

consequence management; and other specialties as determined by the CINC and/or Service and/or DoD Agency sponsoring the assessment.

E3.1.1.27. DoD STANDARD 27: Pre-deployment AT Vulnerability Assessment. DoD Components shall ensure deploying units conduct a pre-deployment AT vulnerability assessment prior to deployment. Commanders shall implement appropriate AT measures to reduce risk and vulnerability. Commanders shall direct AT measures be implemented that reduce risks before, during, and after deployment. If warranted, commanders faced with emergent AT and force protection requirements prior to movement of forces should submit Chairman Combating Terrorism Readiness Initiatives Fund (CbT RIF) requests through established channels to procure necessary materials or equipment for required protective measures. Assessments and the subsequent implementation of standards must occur in a timely manner, and should be incorporated in pre-deployment planning and training. Pre-deployment assessments should assist commanders in updating AOR-specific training and in obtaining necessary physical security materials and equipment to implement protective measures.

E3.1.1.28. DoD STANDARD 28: Construction Considerations. DoD Components shall adopt and adhere to common criteria and minimum construction (i.e., new construction, renovation, or rehabilitation) standards to mitigate AT vulnerabilities and terrorist threats. For further discussion on construction standards, see reference (f).

E3.1.1.29. DoD STANDARD 29: Facility and Site Evaluation and/or Selection Criteria. Commanders shall develop a prioritized list of AT factors for site selection teams. These criteria shall be used to determine if facilities, either currently occupied or under consideration for occupancy by DoD personnel, can adequately protect occupants against terrorism attack.

E3.1.1.29.1. Circumstances may require the movement of DoD personnel or assets to facilities the U.S. Government has not previously used or surveyed. AT standards should be a key consideration in evaluating the suitability of these facilities for use.

E3.1.1.30. DoD STANDARD 30: AT Guidance for Off-Installation Housing. Commanders shall ensure DoD personnel assigned to Moderate, Significant, and High Terrorism Threat Level areas, who are not provided on-installation or other Government quarters, are furnished guidance on the selection of private residences to mitigate risk of terrorist attack. The best protection for individuals is an awareness of the threat and the willingness to take the steps necessary to reduce threat exposure.

E3.1.1.30.1. Residential Security Reviews for Off-Installation Housing. Commanders in Significant and High Threat Level areas shall conduct periodic physical security reviews of off-installation residences for permanently assigned and temporary-duty DoD personnel. Such reviews shall use the same terrorism threat, risk, and vulnerability criteria as that used to assess the safety and security of occupants of other facilities or installations housing DoD personnel on installations within the AOR. Based on the review results, Commanders shall provide AT recommendations to residents and facility owners, facilitate additional mitigating measures, and, as appropriate, recommend to appropriate authorities the construction or lease of housing on an installation or in safer areas.

E3.1.1.30.2. Proper selection of off-installation housing sites can reduce personnel threat exposure. In Significant or High Threat areas, commanders shall ensure the completion of informal residential security reviews prior to personnel entering into formal contract negotiations for the lease or purchase of off-installation housing. The off-installation review should use the same terrorism threat, risk, and vulnerability criteria as that used to assess the safety and security of occupants of other facilities or installations housing DoD personnel on installations in the AOR.

E3.1.1.30.3. Commanders shall include coverage of private residential housing in AT plans where private residential housing must be used in Moderate, Significant, or High Threat Level areas.

E3.1.1.30.4. Commanders at all levels should incorporate family member and dependent vulnerabilities into all antiterrorism assessment, mitigation, and reporting tools. In Moderate, Significant, or High Threat areas, commanders shall include coverage of facilities (e.g., DoD schools and daycare centers) and transportation services and routes (e.g., bus routes) used by DoD employees and their dependents.

E3.1.1.31. DoD STANDARD 31: Executive Protection and High-Risk Personnel Security. Commanders shall be familiar with treaty, statutory, policy, regulatory, and local constraints on the application of supplemental security measures for certain high-ranking Department of Defense officials whom are entitled to additional protection as a result of their position. Commanders shall take measures necessary to provide appropriate protective services for such individuals in high-risk billets and high-risk personnel in their AOR. Review and revalidation of protective services shall occur on at least an annual basis.

E3.1.1.31.1. Commanders should ensure individuals requesting supplemental security measures are aware of constraints and understand their individual responsibilities in accepting additional security measures. Commanders should ensure individuals receiving supplemental security measures have completed required AT training, are cleared for assignment to billets, facilities, or countries requiring such protection, and have been thoroughly briefed on the duties of protective service personnel.

E3.1.1.31.2. Reviews of supplemental security needs should be undertaken within 30 days of a change in the Terrorism Threat Level assigned to an AOR containing high-risk billets or to which high-risk personnel have been assigned.

E3.1.1.31.3. Table E3.T2. associates standards from this Instruction with the existing DoD O-2000.12-H (reference (c)). Using the Handbook should provide commanders sufficient guidance to implement their programs.

Table E3.T2. AT Standards and Associated Chapters/Appendices from DoD O-2000.12-H

DoD Standard	Chapter and Number	Related Appendices
1. DoD AT Policy	Chapter 1	See also Ref (a)
2. Development of AT Standards	Chapter 2	
3. Assignment of AT Operational Responsibility	Chapter 2	See also Ref (a)
4. AT Coordination in Overseas Locations	Chapter 12 -14	
5. Comprehensive AT Development, Implementation, and Assessment	Chapter 4 -13, 15-16	2, 4, 8, 10
6. Antiterrorism Officers (ATOs) shall be assigned in writing at each installation or base, and deploying organization (e.g., battalion, squadron, ship)	Chapter 15	
7. Application of Department of Defense Terrorist Threat Analysis Methodology	Chapter 5	4
8. Threat Information Collection and Analysis	Chapter 5	2, 4, 8, 9, 10
9. Threat Information Flow	Chapter 5	
10. Potential Threat of Terrorist Use of Weapons of Mass Destruction	Chapter 20	
11. Adjustment of Threat Conditions (THREATCONs)	Chapter 6	4
12. THREATCON Measures Implementation	Chapter 6	4
13. THREATCON Measures	Chapter 6	4, 11, 14, 15, 16
14. Commanders shall maintain a comprehensive AT program for their AOR	Chapter 2	22, 23
15. Terrorism Threat Assessment	Chapter 17	2, 4, 8, 9, 10
16. AT Physical Security Measures	Chapter 7	2, 4, 22, 23
17. Terrorist Incident Response Measures	Chapter 17	4, 20, 22, 23
18. Terrorist Consequence Management Measures	Chapter 17	2
19. Training and Exercises	Chapter 20	2
20. Comprehensive AT Review	Chapter 2	
21. General Requirements for AT Training	Chapter 15	
22. Level I AT Awareness Training	Chapter 15	
23. AOR-Specific Training Requirements for all DoD Personnel	Chapter 15	
24. Level II Antiterrorism Officer (ATO) Training	Chapter 15	
25. Training for High Risk Personnel and High Risk Billets	Chapter 13, 15	6, 11, 14, 15, 16, 17
26. Vulnerability Assessments of Installations	Chapter 9, 16	
27. Pre-deployment AT Vulnerability Assessment	Chapter 16, 19	19
28. Construction Considerations	Chapter 9	2
29. Facility and Site Evaluation and/or Selection Criteria	Chapter 10	2
30. AT Guidance for Off-Installation Housing	Chapter 11	2, 16, 17
31. Executive Protection and High Risk Personnel Security	Chapter 13	14, 19